Avant-propos

Poullet, Yves

Published in:
Le règlement général sur la protection des données (RGPD/GDPR)

Publication date:
2018

Document Version
le PDF de l'éditeur

Avant-propos
Le RGPD – une volonté de bien faire : certes ! … mais appropriée ?

Yves Poullet[1]

1. L'ouvrage que vous ouvrez analyse et détricote avec talent chaque ligne d'un texte longuement débattu – jamais un texte de l'Union européenne n'aura subi autant de demandes d'amendements –, d'un texte présenté par d'aucuns comme un monstre, par d'autres comme une simple actualisation de la directive qui l'a précédé[2]. Fallait-il dès lors ajouter à cette réflexion à voix multiples, une introduction ? L'exercice est périlleux. Il ne peut s'agir de résumer les propos d'autrui ni de lancer de nouvelles idées mais plus simplement de s'interroger sur deux points. J'énonce le premier comme suit : « En définitive, quels traits majeurs traversent et justifient ce règlement ? » et le second : « le règlement est-il adéquat par rapport aux défis actuels que le numérique lance à nos sociétés et à nos libertés ? ». La réponse à ces deux questions apportée dans les lignes qui vont suivre n'engage que son auteur. Elle invite au dialogue. Il s'agit bien en ce sens d'une introduction et non d'une conclusion.

[1] Professeur émérite à la faculté de droit de l'Université de Namur, Professeur associé à l'Université catholique de Lille, Membre de l'Académie royale de Belgique.

[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ci-après la « Directive ».

CHAPITRE 1. Les lignes de force du RGPD

2. Quatre lignes de force me paraissent éclairer les dispositions de ce règlement[3]. La première est celle de définir une fois pour toutes, à la face du monde, un modèle européen unifié et cohérent de protection des données à caractère personnel. Ce modèle, c'est sa deuxième vertu, entend prendre en compte les développements technologiques sans précédents intervenus depuis 1995 date de la Directive qu'il a vocation à remplacer, et leur impact sur la protection des données. À cette « révolution technologique », s'ajoutent, troisième ligne de force du règlement, les exigences d'un droit européen qui, depuis 1995, n'a pas hésité à créer un droit quasi-constitutionnel à la protection des données à caractère personnel et que les juges n'ont cessé d'interpréter de manière hardie. Enfin, il n'échappe à personne, quatrième ligne de force, que la préoccupation majeure des auteurs du texte a été de renforcer l'effectivité des règles prononcées.

SECTION 1. – Vers un modèle européen unifié et cohérent : un règlement et non une directive

3. Le choix d'un règlement laissant peu, voire pas de marge de manœuvre[4], et non d'une directive s'explique certes par la volonté des autorités européennes de lutter contre la fragmentation constatée de la mise en œuvre des dispositions nationales nées de la Directive[5]. Le Règlement se veut également bien plus complet et précis que la Directive. Les nonante-neuf articles du règlement remplacent les trente-quatre articles de la Directive. On ajoute à ce premier constat, la volonté de mettre en place un organe unique d'interprétation du règlement autour du désormais « Comité européen de

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ci-après le « Règlement » ou le « RGPD ».

[4] Il en reste cependant. Ainsi, par exemple, en ce qui concerne le régime des données sensibles (art. 9 du RGPD), en matière de presse (art. 85), d'accès aux documents officiels (art. 86), en matière de relations de travail (art. 88). C'est surtout en ce qui concerne l'e-gouvernement, que les États pourront modeler, de manière originale, les traitements du secteur public certes selon des principes communs, et ce en fonction des décisions prises par les instances démocratiques de chaque pays. L'uniformité risque d'être plus présente pour les traitements privés que ceux publics.

[5] Voy. considérant n° 9 du RGPD.

la protection des données », dont les pouvoirs sont sans commune mesure comparés à ceux du défunt « Groupe de l'article 29 » (« Groupe 29 »). La Commission se voit, par ailleurs, déléguer certains actes d'exécution[6], ce qui contribue encore à l'uniformisation européenne de la protection des données. En ce qui concerne la cohérence, l'assignation d'un rôle de *leadership* à une autorité de protection des données en cas de dimension transfrontière d'un problème de protection des données contribue à l'efficacité de l'intervention mais également à sa cohérence. En cas de divergences d'approches entre autorités nationales de protection des données, le RGPD prévoit une procédure qui permet d'assurer l'uniformité de l'interprétation du texte. Enfin, dès avant la mise en vigueur du texte, le Groupe 29 a émis pas moins de neuf « guidelines »[7] qui renforcent l'unité d'interprétation de nombre de dispositions.

4. Ce modèle, l'Europe entend bien l'affirmer à la face du monde. Elle étend le champ d'application du règlement au-delà des frontières en passant du critère flou de la localisation de l'équipement qui permet le traitement, à celui de la cible européenne de l'offre de biens ou services ou du suivi des comportements[8]. Il suffit désormais que le traitement, même piloté hors Union européenne, vise des personnes résidant en Europe pour que la règlementation s'applique. En outre, en matière de flux transfrontières, le Règlement accroît les exigences de protection dite « adéquate », réclamant en particulier l'existence d'une autorité de protection des données. On ajoute toujours à ce sujet que les solutions alternatives, qui pourraient être trouvées afin d'assurer des « garanties appropriées », doivent créer dans le chef des citoyens européens qui en seraient bénéficiaires, « des droits opposables et des voies de droit effectives ».

[6] Art. 92 du RGPD.

[7] Par anticipation du futur travail du Comité, le Groupe 29 a produit des *Guidelines* qui s'emploient à interpréter toute une série de dispositions du Règlement. Avant même son entrée en application, on notait donc la publication (d'avril 2017 à avril 2018) de neuf documents (Privacy Impact Assessment, consentement, transparence, brèches de sécurité, délégué à la protection des données, etc.). Cette efflorescence de documents interprétatifs renvoie au nombre important de concepts flous utilisés par le règlement et accroît la difficulté de lisibilité de ce dernier. Ces guidelines sont disponibles sur le site : http://ec.europa.eu/newsroom/article 29/news.cfm?item_type=1360.

[8] Art. 3, § 2, du RGPD.

SECTION 2. – L'exigence de modernisation de la protection

5. À l'Internet encore balbutiant de 1995, on opposera bien volontiers l'existence désormais d'une toile globale et ubiquitaire, mêlant l'infiniment grand des capacités de nos ordinateurs (le *Big Data*) et de nos réseaux et l'infiniment petit (puces logées dans nos poches, dans nos lunettes, dans les objets voire dans nos cerveaux). C'est l'Internet des objets, les manipulations génétiques, fruits des NBIC[9], le *cloud computing*, l'intelligence artificielle qui déjà fait rêver les transhumanistes voire les post-humanistes[10] et qui, de plus en plus, anime nos robots. Le texte du RGPD entend prendre en compte ces applications nouvelles à travers des précisions à propos des identifiants en ligne et des données de localisation (citées parmi les données à caractère personnel), des dispositions sur le profilage né de l'intelligence artificielle ou encore en évoquant, dans ses considérants, l'application à telle ou telle technologie. Il est certain que l'irruption de ces technologies modifie de manière sensible les modes de collecte, de traitement, de stockage et d'exploitation des données à caractère personnel[11]. Le RGPD fait-il assez et adéquatement, est sans doute une autre question. Nous y reviendrons[12].

6. À la prise en considération des risques suscités par les progrès technologiques, s'ajoute, dans une perspective tout à fait différente, la prise en compte des bénéfices que la technologie peut contribuer à apporter à la cause de la protection des données. À cet égard, on pointe deux principes : le premier est la réciprocité des avantages. Il s'exprime comme suit : dans la mesure où le responsable du traitement bénéficie des applications technologiques pour faciliter son traitement de données, il importe que la personne concernée puisse également faire appel au bénéfice de ces technologies pour exercer ses droits. Ainsi en est-il de l'exercice du droit à la rétractation du consentement, des droits d'information et d'accès qui doivent pouvoir bénéficier des avantages du numérique. Un second principe se déduit des dispositions à propos du « *privacy by design* » ou « *by default* » : l'inscription au cœur du dispositif technique du respect des dispositions légales.

---

[9] Les NBIC désignent des applications nées de la combinaison de diverses technosciences, N : les Nanotechnologies, B : les Biotechnologies, I : les technologies de l'Information et C : les sciences cognitives et ce sur des blocs de matières à l'échelle du nanomètre.

[10] Voire les posthumanistes qui envisagent la fusion des cerveaux humains et de l'ordinateur et l'avenir des robots comme personnes.

[11] Voy. considérant n° 6 du RGPD.

[12] Voy. Chapitre 2, Section 2, *infra*.

SECTION 3. – Les exigences nées de l'évolution du contexte réglementaire et de l'interprétation des juges

7. En 1995, les auteurs de la Directive fondait leur intervention sur la nécessité de créer un marché intérieur de libre circulation des biens, marchandises, personnes, capitaux et services, qui impliquait la libre circulation des données à caractère personnel. L'adoption d'un droit quasi-constitutionnel à la protection des données à caractère personnel à la fois par l'article 8.1 de la Charte des droits fondamentaux de l'Union européenne et par l'article 16, § 1er, du Traité sur le fonctionnement de l'Union européenne modifie la donne et accroit la responsabilité de l'Union européenne de respecter pleinement ce droit, devenu distinct de celui du droit au respect de la vie privée. À cette évolution fondamentale, il faut ajouter les avancées législatives déjà opérées dans le secteur des communications électroniques par la directive *e-Privacy* de 2002[13], déjà remaniée en 2009[14] et actuellement en cours de révision[15]. Ainsi les dispositions sur les brèches de sécurité sont issues de cette directive[16]. On regrette – et nous y reviendrons – que d'autres avancées de cette directive n'aient point été reprises par le Règlement[17].

8. Les juges de Luxembourg n'ont pas hésité, dans le cadre de l'interprétation de la Directive aujourd'hui défunte, à affirmer de manière nette la prévalence de la protection des données sur les intérêts économiques des responsables de traitement (l'arrêt *Digital Rights*[18]), à proclamer le droit à l'oubli et l'extension du champ d'application *ratione loci*

[13] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[14] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

[15] Proposition de règlement du parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), COM(2017) 10 final.

[16] Voy. art. 33 du RGPD.

[17] Voy. Chapitre 2, section 1, *infra*.

[18] C.J.U.E. (GC), arrêt *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, 8 avril 2014, C-293/12.

de la directive (l'arrêt *Google Spain*[19]) et à souligner les limites du pouvoir de la Commission et, à l'inverse, les prérogatives des autorités de protection des données et des juges en matière de flux transfrontières (l'arrêt *Schrems*[20]). Autant de 'leçons' données par les juges qui se devaient d'être reçues par le législateur européen et qui se sont traduites par de nouvelles dispositions.

SECTION 4. – La recherche de l'effectivité des règles de protection des données

9. Lorsque certains agitent l'épouvantail du RGPD, c'est surtout au regard de la situation d'absence, avant son adoption, d'un appareil coercitif lourd et de sanctions prises, sous réserve de quelques exceptions dont il faut bien convenir qu'elles se multipliaient ces derniers temps[21]. Le Règlement entend mettre fin à cette situation en fournissant les instruments de cette effectivité. Un premier moyen a déjà été évoqué : il s'agit de l'approche techno-légale. On épinglera également l'augmentation des droits des personnes concernées, le recours à la 'compliance' interne, le recours à d'autres modes normatifs et, enfin, les pouvoirs de coercition accordés aux autorités de protection des données.

10. L'augmentation des droits des personnes concernées est sans doute une première garantie d'effectivité. Mieux informée, consentant à de meilleures conditions, pouvant exiger de nombreux droits dont notamment celui d'une réponse rapide, celui de l'effacement, d'une information utile en ce qui concerne la logique qui préside à une décision informatisée, il y a fort à parier que la personne concernée exercera plus facilement son contrôle. On ajoute que l'article 80 du RGPD autorise désormais le recours collectif, ce qui ne manquera pas de contribuer à l'augmentation des recours contre des responsables de traitement supposés indélicats.

---

[19] C.J.U.E. (GC), arrêt *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja* González, 13 mai 2014, C-131/12.

[20] C.J.U.E. (GC), arrêt *Maximillian Schrems c. Data Protection Commissioner*, 6 octobre 2015, C-362/14.

[21] Ainsi, la Commission de protection de la vie privée belge, après s'être montrée fort discrète des années durant, s'est décidée à poursuivre, avec succès, devant le juge, Facebook pour pratiques contraires à notre loi de protection des données (Civ. Bruxelles (24e ch.), 16 février 2018, R.G. n° 2016/153/A, disponible sur www.autoriteprotectiondonnees.be).

11. La '*compliance*' interne, c'est-à-dire la mise à charge du responsable du traitement du devoir de veiller au respect des prescrits du Règlement est une deuxième voie de recherche d'effectivité. Elle transparait en particulier derrière l'affirmation du principe d'*accountability* qui exige que ce soit le responsable qui démontre son respect des principes généraux du Règlement[22], par l'obligation de nomination d'un délégué à la protection des données[23], en ce qui concerne du moins certains traitements, ou encore par le devoir de procéder à un *Privacy Impact Assessment* dans certains cas[24].

12. Effectivité toujours, grâce à la mise en évidence de l'intérêt des modes de régulation alternatifs : les codes de conduite, la certification, la labellisation, les ADR[25]. Il ne s'agit pas d'autorégulation à proprement parler, tant le contenu et le déploiement de ces modes alternatifs sont contrôlés par les « gardiens du temple » (les autorités de protection des données), mais d'instruments qui présentent l'avantage, outre celui d'introduire une culture de la protection des données au sein des associations professionnelles, d'ouvrir la voie à l'émergence d'un marché de produits et de services autour de la protection des données à caractère personnel.

13. Effectivité, enfin, par l'octroi à toutes les autorités de protection des données nationales d'un pouvoir de prendre des mesures coercitives[26] et, en particulier, de prononcer des sanctions administratives dont l'ampleur est conséquente[27] pour la vie des entreprises[28]. L'octroi de tels pouvoirs obligera sans doute les autorités de protection des données à jouer un peu moins le rôle de chien de garde prompt à aboyer sans mordre et, vu leur obligation d'intervenir comme sanctionnateur et juge, à mesurer avec prudence les conséquences de leur intervention. On ajoute que leurs décisions pourraient les rendre, le cas échéant, responsables devant les juges pour excès de zèle.

---

22 Art. 5, § 2, du RGPD.

23 Art. 37 du RGPD.

24 Art. 35 du RGPD.

25 « *Alternative dispute resolution* » ou modes alternatifs de résolution de litiges.

26 Art. 58 du RGPD.

27 Entre 2 et 4 % du chiffre d'affaires global, ce qui reste peu par rapport au 10 % d'amendes administratives dans le cas d'atteinte à la concurrence.

28 Art. 63 du RGPD.

CHAPITRE 2. Le RGPD, un règlement adéquat ?

14. Cette deuxième partie de l'introduction se veut plus critique du règlement. Elle opère en deux temps. Le premier collectionne un certain nombre de remarques que je qualifie de pointillistes. Ainsi, la question du consentement, de sa nature et de sa portée mérite quelques réflexions. Je m'attarderai à la définition de la donnée à caractère personnel et à la réglementation peu claire du profilage. Ensuite, je me demanderai, sur la base de quelques dispositions du Règlement, s'il n'y a pas là une invitation à ouvrir à de nouvelles alliances entre le droit de la protection des données et d'autres branches du droit. Enfin, je m'interrogerai sur les raisons de ne pas avoir repris certaines avancées de la directive *e-Privacy*, qui auraient bien mérité d'être généralisées. Le second temps de la critique est plus fondamental : il porte sur la rédaction de l'article 1.2 du Règlement. En définitive, le concept de la protection des données est-il adéquat au regard des enjeux sociétaux du numérique ?

SECTION 1. – De quelques remarques pointillistes

15. Avec raison, les auteurs du Règlement – et depuis le Groupe de l'article 29 – ont renforcé les conditions du consentement, fondement légitime du traitement. Il n'empêche. Faut-il maintenir le consentement comme fondement de légitimité ? Les premières législations (voy., notamment, la Convention n° 108 du Conseil de l'Europe) en matière de protection des données ne l'introduisaient point. On sait que l'article 8 de la Charte le prévoit expressément. Quoi qu'il en soit, je relève que le consentement donné individuellement par la personne concernée reste bien souvent un leurre au regard de la nécessité sociale de l'accès à l'internet et à certains services (les réseaux sociaux, les moteurs de recherche, etc.) : le processus technologique interdit le recul indispensable à une bonne compréhension, à l'heure où la prétendue gratuité du service est avancée comme un bénéfice unilatéral pour la personne concernée et donc mérite en échange la possibilité pour le fournisseur du service à contenu numérique de traiter les données[29]. Ne faudrait-il pas, d'une part, introduire l'idée d'une négociation collective des personnes concernées, via le cas échéant leurs représentants et, d'autre part, en ce qui concerne certains

[29] C'est en tout cas l'idée retenue par la proposition de directive du Parlement européen et du Conseil concernant certains aspects des contrats de fourniture, COM(2015) 634 final,

services de première nécessité évoqués ci-dessus, plaider pour une réglementation *a priori* des traitements nés de leur utilisation ? Au-delà, il serait utile de répondre à la lancinante question : le consentement permet-il au responsable de traiter des données au-delà du principe de la proportionnalité ? En d'autres termes, peut-il traiter, faute du consentement de la personne concernée, de données non pertinentes *a priori* ?

16. Mon deuxième point a trait à la notion de données à caractère personnel qui amènent à mettre en cause cette limite. Deux raisons qui limitent le champ d'application du RGPD. La première renvoie à une idée que j'avais, dès 1979, esquissée à la suite de la lecture de rares législations qui admettaient la protection des personnes morales, protection que la directive '*e-Privacy*' prend en compte. L'asymétrie de plus en plus grande entre le pouvoir informationnel de certaines entreprises qui ont le droit de vie et de mort sur d'autres entreprises, et, précisément, ces dernières, justifient, au nom de la protection de la liberté d'entreprendre mais également de la protection des employés de ces petites structures, que celles-ci puissent bénéficier de certaines prérogatives que le règlement réserve pour le moment aux seules personnes physiques. Une seconde remarque concerne le danger de ne s'attarder qu'aux données à caractère personnel et d'exclure les données dites anonymes dont l'utilisation est de plus en plus fréquente dans les réservoirs de données (les fameux *Big Data)*. Non seulement, Il est loin d'être évident que l'anonymat puisse résister à l'analyse massive et croisée de quantité de données mais en outre, combinées avec des données à caractère personnel, elles peuvent induire, dans des opérations de profilage, des discriminations non seulement individuelles mais également collectives. On note que, dans le cas d'utilisation de données anonymes à des fins de profilage, l'existence de ces catégories de données ne doit pas être révélée alors que leur poids peut être important[30]. À cet égard, l'approche suggérée par la modification de la

9 décembre 2015. Cette proposition prévoit que les utilisateurs des services pourraient légalement conclure un contrat avec le fournisseur, non pas en payant un prix, mais bien en « payant » avec leurs données personnelles ou autres.

[30] Dans son rapport récent sur l'Intelligence Artificielle (*Donner du sens à l'intelligence artificielle (IA)* rédigé par le mathématicien et député Cédric Villani, rendu public le 28 mars 2018 et disponible à l'adresse suivante : http://www.enseignementsup-recherche.gouv.fr/cid128577/rapport-de-cedric-villani-donner-un-sens-a-l-intelligence-artificielle-ia.html), Villani tient le même raisonnement. Réduire la protection des individus à la protection de leurs seules données à caractère personnel n'a plus de sens à l'heure de l'intelligence artificielle et des *Big Data* (p. 148) : « Au regard du développement de l'intelligence artificielle, on peut même se demander si la notion de données à caractère personnel peut tout simplement conserver un sens. Les travaux pionniers d'Helen Nissenbaum nous enseignent par exemple que les données sont des objets contextuels, qui peuvent renseigner simultanément

Convention n° 108 qui définit la donnée à caractère personnel sensible comme toute donnée qui par nature *ou par usage* présente des risques particuliers, m'apparaitrait pouvoir servir d'inspiration pour délimiter la notion de donnée à caractère personnel, ce qui pourrait résoudre ce problème. L'erreur du Règlement est de s'arrêter à une définition certes large mais par nature de la donnée à caractère personnel.

17. Le profilage est évoqué dans plusieurs articles du RGPD : les articles 13, 15 et 22. La question essentielle pour la personne qui se découvre profilée et victime d'une prospection commerciale non désirée ou d'une décision est, au-delà d'une demande de ne plus être profilée ou de refuser que la décision soit exclusivement[31] fondée sur ce profilage, de comprendre les raisons de tel ou tel profilage, d'avoir une transparence de l'algorithme qui conduit à ce résultat et les données retenues au regard des facteurs pris en considération. Or ce point n'est abordé qu'à propos du droit d'accès dans une disposition[32] qui se contente de mentionner que « des informations utiles concernant la logique sous-jacente » seront fournies. N'est-ce pas un peu court, surtout lorsqu'on sait que le responsable du traitement peut encore invoquer le droit au secret ou à la propriété intellectuelle pour réduire l'information utile ? N'est-ce pas un peu réducteur lorsqu'on sait que les entreprises (telles les GAFAM[33], mais également Instagram, Spotify, Snapshat, …) disposant de larges entrepôts de données souvent triviales (comme pour Spotify, la localisation, l'intensité du son, la longueur d'écoute, la fréquence d'écoute, l'heure d'écoute,…) n'utilisent plus une logique *a priori* d'analyse des données, mais construisent leurs profils en confrontant les nombreuses données collectées, à des 'patterns' construits (« *deep learning* ») et revus de manière récursive ? Bref, ces entreprises pourront se targuer de l'absence de logique suivie pour esquiver la demande des personnes concernées.

18. Deux dispositions introduites par le Règlement invitent les défenseurs de la protection des données à chercher des alliances avec d'autres

sur plusieurs individus ou questions. Cela d'autant plus que, dans le cadre du deep learning, les données sont exploitées à grande échelle pour produire des corrélations qui peuvent concerner des groupes d'individus ».

[31] Que veut dire exclusivement ? Il est certain que même si un contrôle humain est prévu, il est rare que le contrôleur ose aller à l'encontre de la vérité sortie des ordinateurs, sous peine par la suite de se voir reprocher son initiative. On note, en outre, que la possibilité de refuser une décision fondée sur un traitement automatisé n'existe que si la décision produit des effets juridiques ou affecte la personne de manière significative. En outre, elle est exclue dans nombre de cas (traitement fondé sur le consentement, nécessaire à l'exécution du contrat).

[32] Art. 15 du RGPD.

[33] Acronyme des géants du Web : Google, Apple, Facebook, Amazon et Microsoft.

acteurs dans d'autres branches du droit. L'une a déjà été évoquée, il s'agit de l'introduction d'une sorte de *class action*, propre au droit de la consommation et reprise fort utilement par le règlement ; l'autre est la disposition relative à la portabilité des données[34] dont l'objectif est certes la protection de la personne concernée, moins enchaînée à son fournisseur de services, que la stimulation d'une saine concurrence, comme cela a pu être décidé en matière de portabilité des contrats de services de communication ou de comptes bancaires. Notre propos est simplement de souligner l'intérêt que pourrait avoir la cause de la protection des données à chercher des synergies avec d'autres branches du droit qui permettront de protéger tantôt la personne concernée considérée comme consommateur face au responsable des traitements bien souvent dans la peau d'un vendeur de biens ou services, tantôt de la protéger contre des abus de position dominante, des concentrations indues sur le marché des données.

19. La directive *e-Privacy* incarne une troisième génération de législation de protection des données. J'ai essayé de le montrer dans un écrit précédent[35]. Sans reprendre le développement, je souhaite m'attarder à deux dispositions y contenues dont on aurait pu souhaiter la reprise par le Règlement. La première concerne l'interdiction, sauf consentement de l'utilisateur, de stocker des informations ou d'accéder à des informations stockées sur l'équipement terminal de l'utilisateur. Ce principe, qui consacre une sorte de droit à la protection de sa maison virtuelle, m'apparaît devoir être proclamé de manière générale comme droit de la personne concernée. La seconde est visée par l'article 14 de la directive et prévoit la définition de normes pour garantir la conformité des équipements terminaux aux exigences de la directive. Cette disposition aurait dû, moyennant adaptation et élargissement, être reprise par le Règlement. Ce dernier n'envisage que la relation entre responsable du traitement et personne concernée. Il laisse dans l'ombre le fonctionnement des terminaux, des infrastructures et des logiciels qui permettent, par exemple, à un site web visité par un lien invisible pour l'utilisateur d'orienter ce dernier également vers un autre site web qui pourra émettre des cookies vis-à-vis du visiteur du premier site ou autre exemple de vendre des émetteurs, récepteurs munis de RFID, avec défaut de sécurité, ce qui permettrait à des tiers d'accéder aux données sur le terminal RFID. En d'autres termes, le Règlement n'entrevoit pas, en dehors de la responsabilité des responsables de traitement, de leurs sous-traitants ou de leurs représentants,

[34] Art. 20 du RGPD.

[35] Y. POULLET, « About e-Privacy Directive. Towards a third Generation of Data Protection Legislation », in *Data Protection in a Profiled World* (GUTWIRTH *et al.* eds), Springer, 2010, pp. 3 à 30.

de responsabilité des producteurs d'infrastructures, de terminaux ou de biens et services comme les logiciels. Le règlement ne prévoit pas, pour ces derniers, de délivrer des équipements conformes ni de systèmes de certification ou de labels de conformité aux exigences de la protection des données. Malheureuse lacune que celle-là. La transparence des traitements ne s'entend-elle pas d'abord de la transparence du fonctionnement de nos équipements ? Comme le note le rapport Villani[36], « une grande partie des considérations éthiques soulevées par l'IA tiennent à l'opacité de ces technologies. En dépit de leur performance accrue dans de nombreux domaines, de la traduction à la finance en passant par l'automobile, il est souvent très difficile d'expliquer leurs décisions de manière intelligible par le commun des mortels. C'est le fameux problème de la boîte noire : des systèmes algorithmiques dont il est possible d'observer les données d'entrée (input), les données de sortie (output) mais dont on comprend mal le fonctionnement interne ». Et plus loin : « En l'état actuel de l'art, l'explicabilité des systèmes à base d'apprentissage constitue donc un véritable défi scientifique qui met en tension notre besoin d'explication et notre souci d'efficacité ».

SECTION 2. – L'article 1er, § 2, du RGPD : un manque d'ambition ? ou une erreur d'approche ?

20. L'article 1er, § 2, du RGPD fixe, de manière laconique, l'objectif du Règlement : « Le présent Règlement protège les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ». Certes, à travers les dispositions du règlement, les personnes concernées voient des limites mises à l'utilisation de leurs données et peuvent réclamer qu'une prévalence soit accordée à leurs intérêts par rapport à ceux du responsable du traitement mais toute pesée d'intérêts exige qu'un critère soit fixé pour opérer cette pesée. Prenons un exemple tiré d'une expérience récente : une compagnie d'assurance me propose une réduction importante de mes primes d'assurance auto, à condition que j'accepte l'installation d'un mouchard dans ma voiture, qui puisse attester de mon bon respect de la législation de circulation routière. Il est vraisemblable que je ne verrai pas d'objection à

[36] Le rapport sur l'intelligence artificielle (IA) rédigé par le mathématicien et député Cédric Villani, rendu public mercredi 28 mars 2018 est disponible à l'adresse suivante : http://www.enseignementsup-recherche.gouv.fr/cid128577/rapport-de-cedric-villani-donner-un-sens-a-l-intelligence-artificielle-ia.html.

une telle proposition, voire que j'y consentirai volontiers. Une question reste cependant : l'enregistrement de telles données est-il compatible avec la conception traditionnelle défendue par le droit de l'assurance, à savoir une certaine mutualisation des risques assurés ?

21. Bref, la pesée d'intérêts peut et doit, dans certains cas, s'opérer non à un niveau individuel mais au regard d'une réflexion de nos sociétés. Cette assertion est encore bien plus fondée lorsqu'on s'interroge sur les traitements de données dans le cadre d'opérations menées dans le cadre de manipulations génétiques, de certains profilages liés à l'octroi de crédit ou d'accès à des soins. En d'autres termes, les débats de protection des données mettent en exergue de manière de plus en plus aiguë, des questions de justice sociale, de dignité au sens kantien du terme, de non-discrimination, etc. L'habitude a été prise ces dernières années par nos autorités de protection des données d'élargir leurs réflexions à ces questions éthiques sociétales[37]. À propos de cet élargissement des objectifs de la protection des données, on opposera à la pauvreté de l'expression retenue par le règlement européen, le texte de l'article 1.1 de la loi française « Informatique et Libertés » de 1978 : « L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

22. Nos autorités de protection des données sont-elles habilitées à instruire et trancher ce type de débat proche d'un *technology assesment* et, le cas échéant, tirer la sonnette d'alarme au nom du principe de précaution ? Ce débat doit être mené[38] et il est certain que nos autorités doivent jouer

[37] Ainsi, le groupe de réflexion éthique mis en place par *l'European Data Protection Supervisor,* les cahiers dits de prospective de la CNIL, etc.

[38] Enfin, on s'interroge sur la possibilité pour nos autorités de protection des données de s'attaquer aux questions fondamentales de société, qui pourtant naissent des développements du numérique sans qu'elle se donne comme grille de lecture, les valeurs de dignité et d'épanouissement de la personnalité, éléments fondateurs du concept de vie privée. L'effacement progressif de la délibération politique par une « gouvernementalité algorithmique », la normalisation des comportements par une régulation technologique insidieuse et ubiquitaire, la prise en compte de plus en plus exclusive de la donnée par rapport au récit et à la rencontre des personnes, les manipulations génétiques et les technologies au service de l'homme augmenté exigent une réflexion plus fondamentale que celle proposée par les législations de protection des données. Que nos autorités de protection des données s'aventurent comme elles commencent déjà à le faire dans ces débats est certes important mais surtout qu'elles ne confisquent pas le débat. Qu'elles le fassent avec les comités d'éthique des sciences, de bioéthique, qu'elles portent le débat chaque fois que cela est utile au public et aux organes de nos démocraties est indispensable.

un rôle même si, nous le répétons, il dépasse de loin le strict débat d'une pesée d'intérêts individuels, seul débat auquel s'attache le Règlement si on suit le libellé de l'article 1.2. Qu'il soit clair que la protection des données n'est jamais qu'un moyen au service de libertés, d'une justice sociale, de la dignité et de la non-discrimination. Reprenons le propos de la loi française. Il affirme clairement le devoir de mettre la technologie au service de l'homme, de son identité, de sa dignité et de ses libertés. Une telle affirmation est également celle de la jurisprudence allemande qui fonde la législation de protection des données sur deux principes constitutionnels : la dignité humaine et l'épanouissement de l'Homme comme être social et de relation. Sans doute, n'est-ce pas le lieu de montrer combien le concept de vie privée, défini par la jurisprudence extensive et créative de la Cour de Strasbourg, correspond à cette approche. On se contente de rappeler le célèbre attendu prononcé par la Cour de Strasbourg dans l'affaire *Pretty*[39] : « Comme la Cour a déjà eu l'occasion de l'observer, la notion de « vie privée » est une notion large, non susceptible d'une définition exhaustive. Elle recouvre l'intégrité physique de la personne (…). Elle peut parfois englober des aspects de l'identité physique et sociale d'un individu (…). Des éléments tels, par exemple, l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle relèvent de la sphère personnelle protégée par l'article 8 (…). Cette disposition protège également le droit au développement personnel et le droit d'établir et d'entretenir des rapports avec d'autres êtres humains et le monde extérieur (…). Bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, la Cour considère que la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8 ».

23. Sans doute, la notion de « vie privée » de par le terme utilisé donne du concept une image bien plus réduite et renvoie à une approche négative, celle de ne pas être vu, de se maintenir en dehors de la société. Telle n'est pourtant pas la signification du concept. La vie privée doit être comprise, non comme une revendication purement individuelle qui exclut autrui, mais au contraire comme celle d'une personne qui réalise son développement à travers tant sa possibilité de retraite en lui-même[40] que son appartenance à la communauté et doit pouvoir ainsi participer

[39] Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 25 avril 2002, req. n° 2346/02, § 61.

[40] Cette possibilité de se retirer « entre les quatre murs de sa maison » mérite sans doute une nouvelle consécration à l'heure de l'ubiquité de l'Internet. En ce sens, on pointe l'idée du droit à l'oubli consacré par le Règlement mais au-delà on s'étonne de ne pas voir consacrer, sans doute avec des limites que la sécurité des tiers et de l'État impose, le droit à un certain anonymat et le droit à la déconnexion.

pleinement et avec son identité propre à la vie de celle-ci comme l'exige notre conception de la démocratie. La protection des données n'est jamais qu'au service d'une vie privée ainsi définie. Cette condition de l'ensemble de nos libertés et de notre dignité doit être rappelée sous peine de voir le Règlement un pur débat de technique juridique sans âme.

24. À cette crainte, s'en ajoute une autre que l'on voit pointer : la protection des données à caractère personnel se mue en propriété des données à caractère personnel. La mutation est insidieuse[41] et a pour elle l'argument que la propriété, concept de droit privé serait sans doute le meilleur rempart de la protection de nos libertés bien publiques. N'est-ce pas en effet dans la transaction éclairée et consciente que l'individu peut décider lui-même de ce qu'il entend faire de SES données ? Cette justification purement individualiste qui, nous affirme-t-on, responsabilise la personne concernée, élude les questions sociétales et de démocratie esquissées ci-dessus ; en outre, elle risque d'accroître les discriminations entre, d'une part, ceux qui souhaiteront pour des raisons de nécessité économique ou sociale, monnayer[42] leurs propriétés au risque de perdre leur âme et, d'autre part, ceux qui attacheront un meilleur prix à leurs libertés. Au-delà, elle introduit l'idée fausse que les données sont le fruit de notre seule action ou décision. Or, les données et l'information qu'elles génèrent sont le produit d'interactions sociales et ne prennent sens que dans le cadre de celles-ci. Peut-être notre propos critique vis-à-vis du RGPD est-il exagéré sur ce point mais le risque est bien là à défaut pour ce dernier de pointer les véritables enjeux des débats de la protection des données à caractère personnel.

25. Pour conclure ces quelques mots d'introduction, il me reste à me faire votre interprète anticipé, cher lecteur. Au terme de votre parcours des quelque 900 pages de cet ouvrage, vous éprouverez, comme moi, un sentiment de profonde gratitude vis-à-vis de ceux qui l'ont dessiné et construit. Vis-à-vis des conceptrices, tout d'abord, Cécile de Terwangne et Karen Rosier, qui ne se sont pas contentées de fixer la route aux contributeurs de l'ouvrage mais les ont guidés par leurs suggestions et leurs conseils. Vis-à-vis de chacun des contributeurs, ensuite, qui se sont efforcés à aller

[41] *Cf.* sur ce point, la tendance relevée par A. Strowel à partir de plusieurs textes récents des autorités européennes à attacher des droits de propriété au sens le plus large aux données ou informations « biens » immatériels au nom de leur valeur (A. Strowel, « Les données : des ressources en quête de propriété », in *Droit, Normes et Libertés dans le cyberespace, Liber Amicorum Yves Poullet* (E. Degrave *et al.* eds), coll. CRIDS, n° 43, Larcier, Bruxelles, pp. 251 et s.).

[42] Et à quel prix… encore faudrait-il qu'ils connaissent la valeur de leurs données pour celui qui les collecte ou les traite.

au-delà du texte pour en traquer toutes les ombres, l'interpréter, le questionner et en mesurer les implications. Sans doute, le RGPD n'a-t-il pas encore livré tous ses mystères mais les clés sont là et je sais qu'elles vous ouvriront toutes les portes.

Bonne lecture.